Safe Cooperating Cyber-Physical Systems using Wireless Communication

Pop, Paul; Scholle, Detlef; Sljivo , Irfan; Hansson, Hans ; Widforss, Gunnar; Rosqvist, Malin

Published in:
Microprocessors and Microsystems

Link to article, DOI:
10.1016/j.micpro.2017.07.003

Publication date:
2017

Document Version
Peer reviewed version

Safe Cooperating Cyber-Physical Systems using Wireless Communication

The SafeCOP Approach

Paul Pop
DTU Compute Dept.
Technical University of Denmark
Kgs. Lyngby, Denmark
paupo@dtu.dk

Detlef Scholle
Alten Sverige AB
Kista, Sweden
Detlef.Scholle@alten.se

Irfan Šljivo, Hans Hansson, Gunnar Widforss, Malin Rosqvist
School of Innovation, Design, and Engineering
Mälardalen University, Västerås, Sweden
{irfan.sljivo, hans.hansson, gunnar.widforss, malin.rosqvist}@mdh.se

***Abstract*—This paper presents an overview of the ECSEL project entitled "Safe Cooperating Cyber-Physical Systems using Wireless Communication" (SafeCOP), which runs during the period 2016–2019. SafeCOP targets safety-related Cooperating Cyber-Physical Systems (CO-CPS) characterised by use of wireless communication, multiple stakeholders, dynamic system definitions (openness), and unpredictable operating environments. SafeCOP will provide an approach to the safety assurance of CO-CPS, enabling thus their certification and development. The project will define a runtime manager architecture for runtime detection of abnormal behaviour, triggering if needed a safe degraded mode. SafeCOP will also develop methods and tools, which will be used to produce safety assurance evidence needed to certify cooperative functions. SafeCOP will extend current wireless technologies to ensure safe and secure cooperation, and also contribute to new standards and regulations, by providing certification authorities and standardization committees with the scientifically validated solutions needed to craft effective standards extended to also address cooperation and system-of-systems issues. The project has 28 partners from 6 European countries, and a budget of about 11 million Euros corresponding to about 1,300 person-months.**

Keywords—cyber-physical systems; systems-of-systems; safety-assurance; wireless communication

I. INTRODUCTION

A *safety-critical system* is a system whose failure might endanger human life or the environment. When a system might harm humans or the environment (or is intended to mitigate or manage such harm), decision-makers require *pre-release safety assurance evidence* that it manages risk acceptably. In some domains, developers prepare an explicit *safety case* combining this evidence with safety arguments, whereas in other domains developers must show that their processes and work products conform to a relevant standard. For the purpose of this document, we call this safety evidence also a "safety case", and the work in SafeCOP applies also for the domains which do not explicitly use safety cases. The conceptual basis for certification is that the pre-release (design-time) evidence anticipates the possible circumstances that can arise from the interaction between the system and the environment, to show that these interactions do not pose an unacceptable risk. Certification is very expensive, and can add a development cost overhead of 25 to 100% [1] and in some cases even 10 times more. For example, "a commonly accepted rule of thumb is that development of safety-certified software costs roughly 10 times as much as non-certified software with equivalent functionality" [2].

If, after performing an initial *Hazard Analysis and Risk Assessment* (HARA), a system is deemed safety-related, it has to be certified. Certification is a "conformity of assessment" performed by a third party: a "certification authority", e.g. an independent organization or a national authority. The certification process depends on the concrete application domain. However, the main ideas are common to all domains. The overall goal is to ensure freedom from unacceptable risk. Safety requirements typically consist of a functional part and an integrity level. A *Safety-Integrity Level* (SIL) captures the required level of risk reduction, and will dictate the development processes and certification procedures that have to be followed, depending on the standard, e.g., IEC 61508 [3], ISO 26262 [4], or RTCA DO-178B [5].

Once a system is certified, the safety certificate is typically valid only for a specific system configuration. This is the case, for example, in the avionics area, where the system is certified as a whole, and even small changes may result in a requirement for complete re-certification. The focus of recent research in safety assurance [6] has been to develop "modular" certification approaches. The idea is that a "modular safety certificate" can be given to an individual subsystem (module), and then these certificates will be manually composed into a system certificate. Thus, when a module is changed, the re-certification efforts can be isolated to the effects of that respective module. Some certification standards, such as IEC 61508 and ISO 26262, allow "modular safety cases" where the safety cases are composed. For example, ISO 26262 has the notion of a Safety-Element-out-of-Context. Recent projects, such as, RECOMP (Reduced Certification Costs Using Trusted Multicore Platforms, EU Artemis JU, 2010–2013) and

SafeCer (Safety Certification of Software-Intensive Systems with Reusable Components, EU Artemis JU, 2011–2015), have proposed modular certification approaches, but these are not yet used in current practice.

II. Cooperative Open Cyber-Physical Systems

SafeCOP addresses safety-related cooperating cyber-physical systems, characterised by use of **wireless** communication, multiple stakeholders, dynamic system definitions, and unpredictable operating environments. We refer to such systems-of-systems as **Cooperative Open Cyber-Physical Systems (CO-CPS)**. We assume that no single stakeholder has overall responsibility over the CO-CPS, that the cooperation relies on the real-time wireless communication to perform a safety-relevant function, and that security issues are of concern. Following the taxonomy of Wilkies et al. [7], SafeCOP targets systems that are of the following three types: (i) use inter-system communication to reach a common goal; (ii) rely on communicated information from other systems in order to ensure safe and/or efficient operation; (iii) provide services that may compromise safety if the communication fails.

Such Cooperative Open Cyber-Physical Systems can successfully address several societal challenges. For example, cooperative vehicles (vehicle-to-vehicle, V2V, and vehicle-to-infrastructure, V2I) have been shown to reduce fuel consumption, reduce the number of accidents (including injuries and fatalities), result in productivity gains and congestion savings, resulting in annual savings of 1,300 to 2,000 billion Euros [8]. The US National Highway Traffic Safety Administration (NHTSA) has estimated that "*V2V safety applications have the potential to address approximately 80% of crashes for unimpaired drivers*". For Road Weather Stations, which is a use case in the project, employing (V2I) and infrastructure-to-vehicle (I2V) communication modes, we can deliver critical up-to-date real-time road-weather data, which can increase traffic safety. In the maritime area, cooperative boats [9] can dramatically increase navigation safety, since, according to the IMO (International Maritime Organization), 75% of ship accidents worldwide are due to human error. CO-CPS can also be employed in the healthcare market, which is characterized by dramatically increasing costs. For example, cooperative robots can be used to reduce the amount of physical labour in hospitals. The use cases (UC) addressed in the project are summarized in Figure 1. In the remainder of the section we briefly summarise each of the use cases.

In UC1 we will develop a two-robot autonomous bed mover that can wheel ordinary hospital beds through the cluttered and populated corridors without causing hazardous situations. The system will be developed so that neither the robots nor the bed between them shall cause a collision. The corresponding safety assurance case will consider both the system failures as well as behaviours of the system in case of external emergencies. Guaranteed reliable communication is essential for both the basic behaviour and the response to external problems.

In UC2 we develop methods and tools for a proof-of-concept system where (semi-)autonomous boats and other vehicles cooperate to perform bathymetry measurements for a portion of a port. For example, an autonomous UAV cooperates with the boats, flying over the area providing communications and coordination functionalities, increasing reliability, resilience and flexibility of the system. The proof-of-concept system will be capable of collecting sensor data, identifying obstacles and providing reliable route planning/changing.

The goal of UC3 is to demonstrate how we can apply and extend safety assurance frameworks to automotive cooperative safety critical V2X-based systems. This class of systems presents new challenges such as security implications on safety. In UC3 we will develop a Control Loss Warning system for a vehicle platoon such that if a vehicle in the platoon loses some functionality affecting the platoon, all vehicles downstream and the road infrastructure are notified so that they can perform appropriate and coordinated actions.

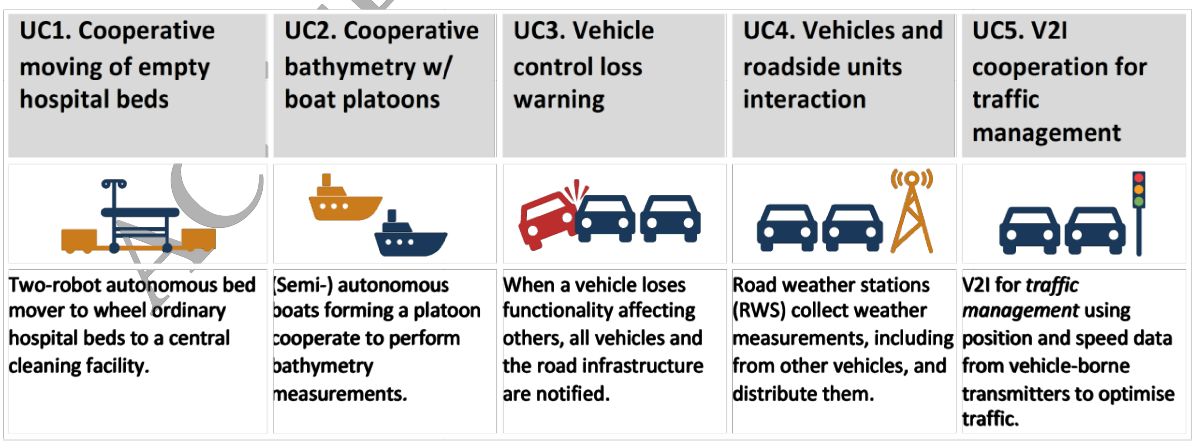

Figure 1: Use cases addressed in the project

In UC4 we focus on the interaction between vehicles and roadside units (RSU). RSUs are typically installed to the fixed locations besides the road. A special case of RSUs are the road weather stations (RWS), which collect different measurement parameters related to the weather and traffic, and deliver this data to a single data collection point. Typically, this data is delivered to a road administrator that forwards it on to TV and radio stations. In SafeCOP we will extend the responsibility of the RWS to also deliver the data directly to the passing vehicles. Moreover, the vehicles can also act as data collectors and forward their weather and traffic data back to the RWS. To ensure purity of the delivered data and the communication session, sequential validation checks and continuous observations are required through a runtime manager.

In UC5 we focus on the Intelligent Transportation Systems (ITS) aimed at improving transportation efficiency and safety. More specifically, we look into an integration of the Adaptive Traffic Light System (A-TLS) and Green Light Optimal Speed Advisory (GLOSA) applications. A-TLS adapts its signal plan to the changing traffic conditions, while GLOSA informs vehicles drivers about the optimal speed they should maintain in order to arrive at the intersection when the light is green. UC5 explores the integration of the integrated traffic management application and a Video Content Analysis (VCA) platform for detecting possibly dangerous road events/situations. Such integrated system contributes to the active road safety, in order to alert drivers of different traffic anomalies.

The development CO-CPS poses challenges that are not adequately addressed by existing practices nor standards. While careful safety-aware design and thorough safety assurance is required, no single manufacturer has design authority over or responsibility for the safety of a set of cooperative embedded systems. Developing a safety critical system typically requires making design decisions that trade-off safety concerns, functionality, cost, and other considerations. Achieving adequately safe cooperative cyber-physical systems requires arriving at, realising, and assuring a safe design even though participants in the design process are competitors reluctant to share all of their concerns or intricacies of designs with each other. Moreover, due to the cooperative and openness nature, many circumstances which have to be covered by the pre-release safety assurance are difficult to anticipate at design time in the case of CO-CPS.

III. Project Objectives

The concrete objectives of SafeCOP are:

- **Objective 1**. *Develop a safety-assurance framework for CO-CPS*. The primary objective of SafeCOP **is to** propose an approach to the safety assurance of CO-CPS which will facilitate their certification and market release. This will create new applications and market segments, successfully addressing societal challenges.
- **Objective 2**. *Develop a reference "Runtime Manager" architecture to support the engineering and certification of CO-CPS*. SafeCOP will define and develop a reference "Runtime Manager" (which extends the reference platforms in the targeted application areas) that detects at runtime abnormal behaviour, triggering if needed a safe degraded mode. The verification, validation and simulation methods and tools developed as part of Objective 1 will be used to produce, besides the safety assurance evidence needed to certify cooperative functions, also the conditions that need to be observed by the Runtime Manager to ensure safety.
- **Objective 3**. *Extend the current wireless protocols for safe and secure cooperation*. SafeCOP will evaluate the adequacy of standard wireless technologies for CO-CPS to be used in the target application areas, and will propose an application-level "safety layer" on top of existing protocols to ensure safe and secure cooperation such that CO-CPS can be certified.
- **Objective 4**. *Contribute to new standards and regulations*. An important objective of SafeCOP is to contribute to new standards and regulations, e.g., provide the certification authorities and standardization committees with the scientifically validated solutions they will need to craft effective standards which have been extended to address cooperation and system-of-systems issues.
- **Objective 5.** *Demonstrate the usefulness of SafeCOP concepts in target applications.* We take five real-world applications in several domains and build demonstrator systems which show how CO-CPS can have concrete utility across a broad range of real commercial applications.

IV. Concept and Approach

Figure 2 presents the SafeCOP safety assurance concept. The approach in SafeCOP is to *restrict the behaviour* of the cooperative safety function at *runtime*, such that the *design-time* safety assurance evidence, with additional *monitoring at runtime*, is able to guarantee the safety requirements. Such an approach may require changes to the certification standards, hence the objective to contribute to new standards and regulations. Standardization will be prompted by the SafeCOP project partners that are *safety assessors* (DNV GL, Safety Integrity, DTI), as well as members of standards committees. Additionally, the project is strengthened by an external advisory board, comprising people with vast safety assurance and security-related expertise. They will make sure that the innovations developed in SafeCOP are grounded in current certification practice and are aligned with the current efforts in the tech-

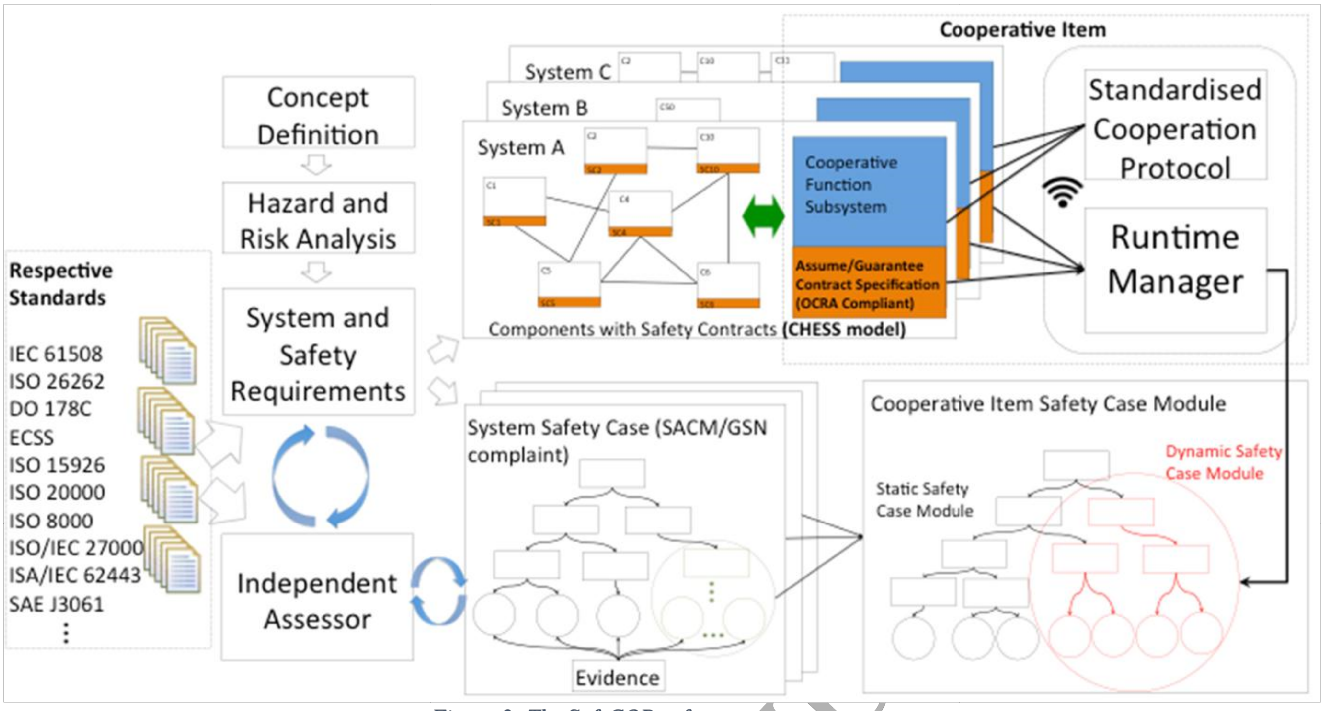

Figure 2: The SafeCOP safety assurance concept

nical committees tasked with extending the certification standards. The evaluation of the proposed framework will be available in the SafeCOP "Deliverable D5.9 Evaluation of the SafeCOP approach as shown by the demonstrators"[1].

Figure 2 shows three CPS systems, A, B and C, developed by three different organizations. Note that the systems (actually Systems-of-Systems) addressed in SafeCOP may consist of several cooperating cyber-physical systems where each of those systems has its own accompanying safety case. Each system has a cooperative subsystem co-responsible for the cooperative safety function, referred to as a cooperative item in Figure 2. In SafeCOP we consider that the design, or even implementation, of certain subsystems of the cooperative item are developed independently of the systems in which they are used (e.g., systems A, B, and C). Such independent development of safety-relevant subsystems is supported by different standards, e.g., in ISO 26262 through the notion of Safety Element out-of-Context (SEooC). In SafeCOP we intend to use contract-based design to facilitate the independent development of cooperative safety functions. We will build upon results on contract-based design from ARTEMIS projects such as CHESS [14] and CONCERTO [15], which focused on developing the Chess-toolset [16]– a tool for model-driven and component-based development of high-integrity systems. The components in the Chess-toolset can be annotated with assumption-guarantee contracts and verified using the OCRA tool [17] for checking contract refinement. In SafeCOP, we will use such contracts for both design-time and runtime contract checking. Our solution in SafeCOP is to enrich the Chess-toolset by providing support for development of CO-CPS. More specifically, the tool will distinguish between the runtime and design time contracts and tightly couple the contracts with the corresponding safety assurance evidence to address the dynamic safety assurance nature of CO-CPS.

The communication between the different CO-CPS in our cooperative item is wireless. The wireless communication subsystem is an example of an independently developed safety-relevant element that is a part of the cooperative item. SafeCOP will extend the current state-of-the-art wireless protocols by creating an application-level library and related API that acts as a "safety layer" on top of the existing protocols. If this API is used for the communication, we guarantee that the communication has "high integrity", i.e., trust is provided that the contents of messages are not corrupted either unintentionally or intentionally. This is needed because otherwise our cooperative function A cannot trust messages from the other systems (B and C) to implement its safety function. In providing such high-integrity communication, we will in addition to considering traditional safety concerns, reuse security results from other ARTEMIS projects such as DEWI and from the Cooperation Reference Technology Platform (CRTP), and our focus is on delivering a solution that is not susceptible to security threats, such as man-in-the-middle attacks. Considering security is essential, as security concerns are not covered in detail in current safety standards, potentially resulting in systems that are successfully certified according to relevant safety standards, but that still are open to security threats that may jeopardize safety.

Traditionally, an organization prepares their safety assurance evidence for the safety case at design-time. The notion of a cooperative item extends the scope of the safety case from a single system to other systems that are not necessarily known during

[1] Public Deliverables: http://www.safecop.eu/?page_id=66

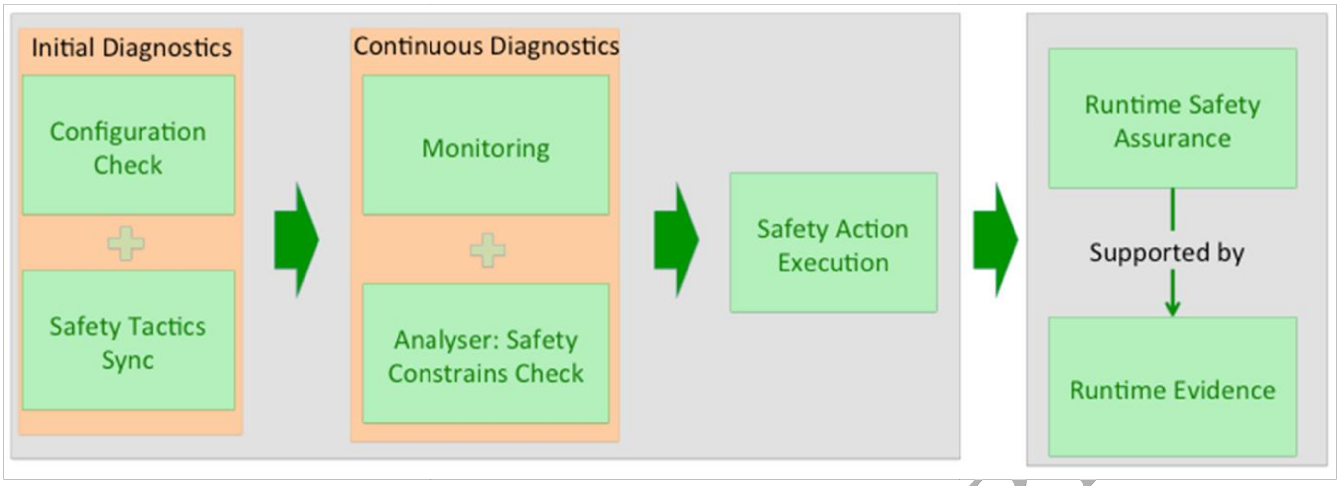

Figure 3: The SafeCOP Runtime Manager concept for CO-CPS

design time. To provide additional assurance of such open systems, runtime safety assurance supported by runtime verification is also required. In SafeCOP, the safety case of the system A prepared by organisation A includes a safety case module related to the cooperative item, which covers not only the system A, but also the cooperating systems B and C. Since each organization is interested in protecting their Intellectual Property (IP), it is not always practically feasible to include the detailed evidence from other organizations. Hence, in SafeCOP, the cooperative item safety case module prepared by the organization A is done by composing the evidence of the cooperative subsystem A with the public evidence from the cooperative subsystems B and C (i.e., without exposing the IP of the organizations B and C). This is similar to modular certification allowed by certification standards, e.g., SEooC. The difference is that modular certification typically does not hide the IP and does not address runtime safety assurance. We also refer to this as composing safety cases, since the safety case for the cooperative item will be based on the individual safety cases for subsystems A, B, and C.

Runtime diagnostics is a part of most modern safety-critical systems [21]. In SafeCOP, we extend the traditional runtime diagnostics with a Runtime Manager (RM) for cooperative cyber-physical systems. Complementing the diagnostics, RM works on an extended scope of variables that affect the runtime behaviour and establishes runtime certificates ensuring compatibility of the CO-CPS. The SafeCOP Runtime Manager for CO-CPS concept is shown in Figure 3. RM first ensures that all the cooperating systems contain a compatible cooperative item subsystem and that the configuration of the cooperating systems is within the predefined values established during out-of-context development of the cooperative item. One of the roles of RM will be to synchronise the safety tactics amongst different cooperating systems to ensure that their behaviour in safety-critical situations is compatible.

The safety case relies on constraints that restrict the runtime behaviour of the safety function, in order to anticipate at design time the circumstances that can occur at runtime. These runtime constraints are derived from the safety requirements and are enforced by the RM, which includes monitoring of the cooperative safety function. RM checks the safety constrains in terms of assumption-guarantee contracts during runtime, and generates runtime evidence. The dynamic part of the safety assurance case is built upon the runtime evidence. Since such evidence is tightly coupled with contracts, the resulting safety assurance case depends on the satisfaction of the contract assumptions. We call this a “conditional safety case”: the safety requirements are guaranteed by the contracts only if the demands in terms of contract assumptions are satisfied. For example, the integrity of cooperative subsystem A is guaranteed by system A’s *architecture* and safety mechanisms. The public safety evidence of the subsystem B is refined into a set of *demands* that have to be fulfilled by subsystem B in order to ensure its integrity. In SafeCOP, we will use the OMG standard SACM (Structured Assurance Case Metamodel) [20] for modelling the safety case. The SACM framework supports both main graphical assurance case notations: Goal Structuring Notation (GSN) [19], and Claims Arguments Evidence (CAE) [18]. The standardisation and portability offered by SACM enables frequent updates to the safety case with less effort, as it becomes easier to automatically update the dynamic safety assurance case.

If the Runtime Manager detects abnormal behaviour, or if the demands are not satisfied, the cooperative safety functionality is disabled. RM is responsible for the safety action execution. SafeCOP will analyse the requirements of the use cases and propose constraints based on the definition of the cooperative safety functions, such that safety is guaranteed. The safety case needs to also consider the risk of requirement violations, and how to provide failsafe fallback mechanisms. Considered mechanisms, including safety under such scenarios, will introduce additional constraints on the systems involved.

The Runtime Manager is implemented as software that needs to run on the CO-CPS system to ensure safe cooperation at runtime. This RM has to be “separated” from the functionality of the device, such that lower-criticality functions do not affect the

functioning of the high-criticality RM. Some platforms (e.g., AUTOSAR[2]) provide such separation mechanisms, but some (such as ROS[3]) do not, so these separation mechanisms (similar in concept to a "virtual machine", but more lightweight) will also have to be developed. The RM has to know what to monitor; the "Verification and Validation" methods and tools will produce safety requirements that need to be monitored at runtime. Once the RM detects a safety violation, it will have to fallback to a "degraded mode". The functionality of the "degraded mode" will have to be developed in the demonstrators, and it is specific to the function of the respective demonstrator. It is challenging to develop useful and failsafe fallback functions, since often it is not appropriate to just stop (assuming there is a "safe stop" function).

The Runtime Manager contains a *monitoring module* that performs *data acquisition* to collect safety-related data, which is then analysed and included in the safety assurance evidence. In this context, we say that we have a "living safety case", which is updated with information collected at runtime to increase confidence. In this context we also say that the safety case is *incremental*, and it may support *provisional certificates* allowing usage in limited scenarios (e.g., initially only in-the-lab use). Through evidence collected at runtime, provisional certificates can be upgraded to cover more general usage scenarios. The qualification of the Runtime Manager and the constraints are part of the design-time safety assurance evidence.

A. *Dependable wireless communication*

SafeCOP focuses on safety assurance for cooperative CPSs that communicate through a wireless channel. It is therefore crucial to thoroughly investigate the wireless communication behavior in a CO-CPS application to make sure that uncertainty pertaining to wireless signal propagation and networking protocols are well taken into account and do not compromise CO-CPS safety requirements [22]. There are several wireless networking technologies designed for short-range communication (IEEE 802.15.4, Bluetooth, ZigBee, WirelssHart, 6LowPAN), medium range communications (IEEE 802.11 and its variants) and long-range and broadband communications (GPRS, 3G/4G, LTE, WiMAX, etc.). The challenges of using wireless technologies in safety critical applications are currently being addressed in large ARTEMIS projects such as DEWI, which declares that "*current wireless technologies […] still lack features like composability, dependability, security, safety, privacy and auto-configuration. Furthermore, current solutions do not have a common reference design and service-oriented architecture that would be needed to build a market environment where competition enables lower prices*"[4]. As the wireless cooperation will have to meet strict real-time safety requirements, to achieve the composability with respect to the temporal behavior, time-triggered communication is required [23]. The challenge of securing such time-triggered wireless communication is being addressed in the RETNET project.

SafeCOP contributes to providing innovative communication protocols based on COTS standard wireless technology and state-of-the-art from projects such as RETNET, to ensure safe and secure cooperation in CO-CPS applications. Indeed, the diversity of use cases to be implemented and deployed within the SafeCOP framework including automotive, maritime and healthcare domains requires that different wireless communication technologies be investigated for both short-range indoor and long-range outdoor communication patterns with a particular focus on their safety-related features. The use of wireless communication technologies for integration of heterogeneous CO-CPS represents a major added value of the SafeCOP project that will advance the current state-of-the-art solutions. Furthermore, the study of the capabilities of these COTS technologies with respect to safety assurance and certification is a new challenge addressed in the SafeCOP project. Considering that SafeCOP uses standard technologies, it will contribute to devising new extensions to existing wireless communication standards to cope with safety requirements for safety-critical CO-CPS applications. These contributions may be considered in the release of new standard protocols for safety critical CO-CPS as SafeCOP partners will work closely with standardization bodies.

V. Work Packages

As the central goal in the project is to provide an approach for the safety assurance and engineering of cooperative open cyber-physical systems (CO-CPS), we have organized the project around a number of use cases that feed requirements and problems into the research work-packages (WPs). The proposed solutions are then demonstrated and evaluated to ensure the feasibility of the approach.

The project is organized in seven WPs:

- WP1. Requirements,
- WP2. Safety assurance framework for CO-CPS,
- WP3. Safe and secure wireless cooperation,
- WP4. Platform and tool support for safety assurance,
- WP5. Demonstrators and evaluation,

---

[2] http://www.autosar.org
[3] http://www.ros.org

[4] https://www.thalesgroup.com/en/spain/event/tas-e-participates-project-dewi-dependable-embedded-wireless-infrastructure-under

- WP6. Dissemination and exploitation,
- WP7. Management.

The research and innovation work in the project is defined by the requirements derived in WP1. These requirements are coming from the use cases, which are part of the WP5 on demonstrators and evaluation. In WP1 we do the collection, refinement and consolidation of the requirements and research drivers. These consolidated requirements and research questions are then the basis of the work of WP2, WP3 and WP4, which provide solutions that—in turn—are applied and evaluated in several demonstrators in WP5. WP2 is concerned with the development of the SafeCOP safety assurance framework targeting CO-CPS, which communicate wirelessly. The wireless communication is addressed in WP3 where the goal is to extend the current protocols such that they provide the required levels of safety and security for CO-CPS. The safety assurance framework is supported by the SafeCOP platform, which consists of reference architecture for CO-CPS and methods and tools for producing safety assurance evidence. The work in WP2, WP3 and WP4 is performed in parallel, with interactions on the issues related to the assurance framework, wireless protocol, architecture and methods and tools. All WPs are structured such that intermediate evaluation of the approach is possible every year. WP7 is responsible for ensuring and monitoring the collaboration as described above; all WP leaders are part of this task. The dissemination of the major findings of the project will be done in WP6, and the management activities in WP7. A description of each WP follows.

WP1 Requirements. The goal of this work-package is to establish both the business case of the approach as well as the requirements for the solutions as they apply to different domains. The business cases establish goals that have to be achieved, and that can be assessed in the evaluation work-package (WP5). The requirements provide the specific constraints and problems that have to be solved in work packages WP2, WP3, WP4. The focus of WP1 is on safety and security related requirements for the implementation of cooperative safety functions required by the use cases.

WP2 Safety assurance framework for CO-CPS. The main objective of this work package is to develop a practical safety assurance framework for CO-CPS. After an evaluation of the state of the art on safety assurance, the WP proposes an assurance framework that can address the challenges of CO-CPS by combining pre-release safety assurance with runtime monitoring. The basis for this framework is a composable safety case, which contains "demands" placed on cooperative subsystems in order to provide safety "guarantees" for the cooperative safety function. In this WP we also evaluate and extend a safety analysis method called STAMP, which is suitable for systems with a lot of interactions. This work package also produces a set of scientifically proven recommendations for the certification of CO-CPS.

WP3 Safe and secure wireless cooperation. In SafeCOP we address cooperative open systems that communicate using wireless technologies. We are interested to elevate the state-of-practice to develop technologies that are both safe and secure, to be used in the context of CO-CPS. Hence, we start by evaluating standard wireless technologies that can potentially be used for cooperative safety functions, and we extend these wireless technologies to ensure and facilitate assurance of safety and security in cooperative embedded systems. Once a safe and secure communication solution is available, in this work package we are also interested to design distributed cooperation algorithms with safety-critical requirements.

WP4 Platform and tool support for safety assurance. The goal of this work package is to provide a platform and tool support for safety assurance. The WP defines a reference platform (hardware, OS and middleware), with the aim to guarantee the integrity of the cooperative function. We will extend the major platforms from each application area, e.g., AUTOSAR for automotive and ROS (which lacks safety mechanisms) for mobile robots. The novel component in the platform is a Runtime Manager, which enforces the cooperative function safety requirements providing a failsafe state in case of failure. This work package also extends the ARTEMIS Reference Tools Platform, with a focus on extending tool flows to support in efficiently producing safety evidence for certification.

WP5 Demonstrators and Evaluation. The consortium develops a number of demonstrators based on the use cases presented in Figure 1 to show the applicability of the approach in different industrial areas. The demonstrators are built using the wireless technologies, platforms, methods and tools in WP3 and WP4, by applying the safety assurance process developed in WP2. This work-package also evaluates the results of the demonstrators. Both the work packages and the demonstrators will be subject to evaluation that will be reported in the publicly available D5.9 deliverable mentioned in Section IV. Furthermore, WP5 provides various requirements input to WP1, and provide feedback that can be used to guide further research and development work in work packages WP2, WP3, and WP4.

WP6 Dissemination and exploitation. All partners advertise SafeCOP to their networks; academic, industrial, business or general public. This work-package includes setting up the project web site, producing newsletters, organization of workshops, demo booths, etc. An important component is also to liaison with standardization organizations to provide information about the results of the project. The objective of the exploitation phase is to identify and implement the actions necessary to maximize the market value, the business potential and the social benefits for the European Union of the project outcomes. The phase will be carried out using the consortium's networks and other channels to explore vertical applications, use cases and disseminate commercially the solutions developed within the project. The exploitation will also address the standardization activities: the definition of new

standards for safety requirements and the specification of methodologies for testing and compliance to the SafeCOP concept, will represent an important achievement/highlight of the project.

WP7 Management. This work package contains all tasks related to the management of the project, i.e. monitoring and reporting. Central to the success of the project will be the establishment of a good quality plan, risk management plan and communication plans to ensure good information flow between the partners. Moreover, this work package also includes knowledge and Intellectual Property Rights (IPR) management in the project.

VI. Consortium

The consortium is industry-led, consisting of 7 Large Enterprises, 10 Small and Medium Enterprises (SMEs), working with 6 universities and 5 Research Transfer Organisations. The partners are positioned across the full value chain, from technology providers, to system integrators, OEMs and end-users. The presence of 3 safety assessors and 6 members of standardization bodies facilitates the exploitation of safety assurance results. As already mentioned previously, beside the stakeholders represented by ECSEL JU monitoring the project, the project established an advisory board.

Special emphasis is taken on a balance between technology users and providers on the one side, and large companies, SMEs and researchers on the other. This balance will facilitate the technology transfer from theory into industrial practice. Particular emphasis has been put on the integration of SMEs. This can be seen on the quality and number of SMEs involved in the project. The enterprises (SMEs and LEs) include Original Equipment Manufacturers, system integrators, and end-users.

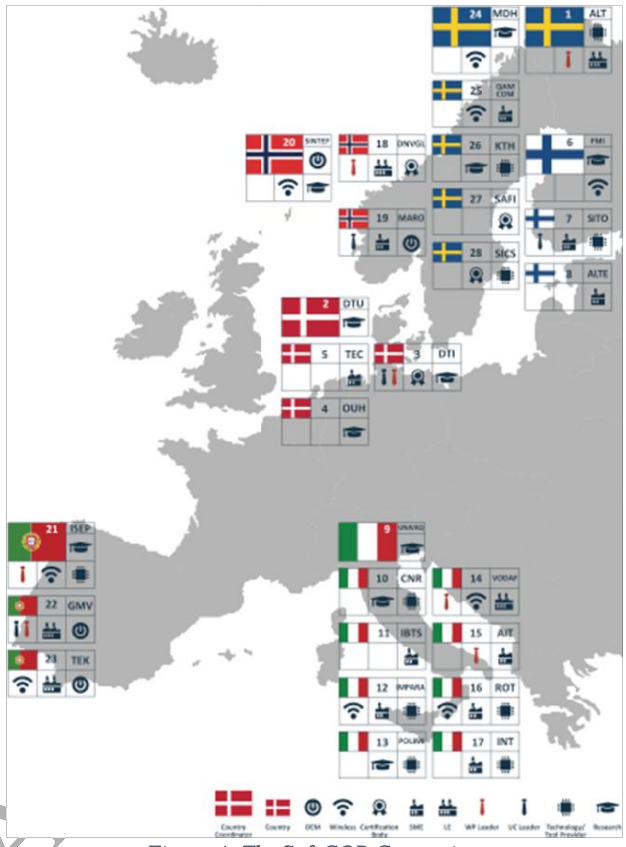

Figure 4: The SafeCOP Consortium

The project partners are from six European countries, with four representatives from the Nordic countries (Denmark, Finland, Norway and Sweden) and two from Southern Europe (Italy and Portugal). An overview of the number of partners per country can be found in Figure 4.

The project coordinator is Alten Sverige, a Sweden-based LE with a presence in 20 countries. The LE's (Alten Sverige, DNVGL, GMVIS Skysoft, Intecs, Odense University Hospital, TEKEVER Autonomous Systems and Vodafone Automotive Italy) and SMEs (ALTE Visetec, Aitek, Impara, Intelligence Behind Things Solutions, Maritime Robotics, SITO, Qamcom Research & Technology, Ro Technology, Safety Integrity and Technicon) in the project cover several market domains with representatives from the automotive, maritime and healthcare sectors. Their presence ensures that the five use cases are properly grounded, that solutions are business-oriented, and that the final exploitation of the results reaches the right groups across multiple domains.

Having experience with nationally co-funded projects where a whole country has had to drop out, we have organised our five demonstrators in national units bound together by an international research "cap" with sufficient redundancy in expertise to cover the withdrawal of a single country if need be. Each of the national units are partners who have worked successfully together before, though not all on the same projects, and all of the university researchers involved have worked together previously in various subgroup combinations. All of the university partners and most of the industrial partners have previous experience with both national and international research projects, although three of the partner departments have not been involved in European projects before.

A. Setting up the consortium

The ARTEMIS and ECSEL funding instruments have promoted the assembly of very large and complex projects, often involving more than 100 person years, 8-100 partners and a (public) budget of between 0.4-42 million Euros. The average project has 25 partners and 9 million Euros total budget [10]. The strategy is to "think big" to gain "impact" and even if it is not primarily the size of the consortium that is meant, it is still an underlying message, that the larger it is, the more impact it will have. "The ARTEMIS mantra 'think big' does not mean that all projects have to be huge ones like the ARTEMIS CESAR project (Cost-efficient methods and processes for safety relevant embedded systems), which has about 58 partners and about €68 million of investment, it means thinking about the impact that the project will have" [11]. The dimension of the projects poses several challenges for its management. Hence it is not likely that all the staff from two partners ever meet in the project. The policy of promoting large and complex projects is also reflected in the support for proposal that is available in the ARTEMIS consortium-building events.

New proposals are fostered at brokerage events, where new ideas are exposed in plenum pitches with hundreds of present representatives from industry and research. At breakout session all interested potential partners are welcome. There is no mechanism to allow the consortium leader to sort out undesired partners. The worst scenario is to walk off with 30-40 interested organisations, all of them expecting to be part of the proposal; limiting the consortium is a difficult task.

The funding of ARTEMIS/ECSEL is a blend of European contribution and contributions from each national innovation agency [12]. Each national agency has its own criteria and rules for payment. Most countries ask for an industrial project leader, and a specific budget ratio between industry and academia. That means that one prospective academic partner often has to find one or two other partners from the private sector to be nationally eligible. This means that the consortium will grow at least one extra round, without any real chance for the consortium leader to control the development.

Specific challenges are: the risk that large segments of partners or sub-clusters fall away, including valued partners, the risk that some sub-clusters cannot create eligible national consortia, and when some countries choose not to fund a specific project, or otherwise run short on budget—or, frankly, stop supporting the funding scheme.

A structured semi-open methodology. We have had experience with such a *snowball processes* several times before. To take the lead and propose a topic and gather a consortium is not an easy task in a very open environment. As an alternative to the "snowball strategy", we performed a more structured process in the SafeCOP proposal. That fosters narrower, smaller and (we believe) better consortia. The objectives for this are to gather a large group of interested potential partners, but through the process select the most desired ones.

We first proposed our SafeCOP project at a consortium-building event, early in February 2014. In this case we presented the project in a five-minute pitch talk, together with 50 other presenters in a plenum session. We also presented a poster, and the project was also posted on the web a couple of weeks ahead. The result was a list of 37 interested individuals, representing 31 different organisations, where 4 were large companies or industries, 6 SMEs, 12 institutes and 9 universities, from 14 countries. The "usual" process would be to use the breakout sessions to form an initial outline of the proposal, and start assembling the consortium.

But for us, the next step was to contact the 37 person large group after two weeks. The message was that we planned to form a consortium out of the group of interested partners. They were all given the task to describe (1) their own organisation, (2) what their contribution would be and (3) whether they would be willing to lead any task. They were given a three-week deadline. The result was a detailed list of potential partners, but the list had been shortened to 10 potential partners, of whom 1 was from industry, 2 from SMEs, 3 from institutes and 4 from universities, from 10 countries. We believe that the action sorted out the better half of the list—those who were actually responsive to joint actions.

At the end of the day eligible country consortia are needed in this kind of call, and therefore the next step was to ask the 10 interested potential partners to provide national rules for the call (if known), and also to propose additional potential partners from their own country *if needed*, with respect both to national rules and the direction of the proposal. The potential partners had one week to suggest partners and another week to get the same kind of information from these new, suggested partners. At this stage at least one country left, but also one new entered. The result was a detailed list of potential partners, but the list had been extended to 26 potential partners, of whom 5 were from industry, 8 from SMEs, 7 from institutes and 6 from universities, from 10 countries.

Thereafter we selected three core partners, from three different countries (Denmark, Italy and Portugal); however, the Italian company could not commit itself at this stage. The core team worked out a "write-up" and selected partners and partner countries, mostly from the set of already interested partners, but also some totally new ones, that fitted into the project. Now the first revision of the consortium was Sweden, Denmark and Portugal, plus Norway, the Netherlands and Germany. In addition, Austria was asked to join. A message was issued for all the interested organisations that they were currently not included, but that they might be taken into account at a later stage. At this stage Italy re-entered into the consortium, while Austria, the Netherlands and Germany fell away.

We have established this way of working to find better ways to establish new European research consortia. First, we identify *la tête de la course*, as a core team, and then we pick the breakaway specialist out of the bunch of the platoon—using a sports idiom. In this "marathon methodology" we try to select the best of those who want the most, to form a winning team.

VII. Conclusion

This paper has presented the SafeCOP ECSEL project. We have covered the societal challenges addressed, the project objectives, the overall approach and the consortium formation process. As mentioned, SafeCOP targets safety-related Cooperating Cyber-Physical Systems (CO-CPS), where no single stakeholder has the overall responsibility over the resulted system-of-systems; safe cooperation relies on the wireless communication; and security is an important concern. Although such CO-CPS can successfully address several societal challenges, and can lead to new applications and new markets, their certification and development is not adequately addressed by existing practices. Note that many of the research and innovations of SafeCOP also apply to CO-CPS that are not safety-related.

SafeCOP brings clear benefits in terms of cross-domain certification practice and implementations of cooperating systems in all addressed areas: healthcare, maritime, vehicle-to-vehicle and vehicle-to-infrastructure (V2I). The advantages include lower certifi-

cation costs, increased trustworthiness of wireless communication, better management of increasing complexity, reduced effort for verification and validation, lower total system costs, shorter time to market and increased market share. The results are demonstrated in five demonstrators: cooperative moving of empty hospital beds, cooperative bathymetry with boat platoons, vehicle control loss warning, vehicle and roadside units' interaction and V2I cooperation for traffic management.

ACKNOWLEDGMENT

The research leading to these results has been performed in the SafeCOP-project, that received funding from the ECSEL Joint Undertaking under grant agreements n°692529, and from National funding.

REFERENCES

[1] IBM Software Rational, "DO-178B compliance: turn an overhead expense into a competitive advantage", White paper, 2010.

[2] K. Nilsen. "Certification requirements for safety-critical software." RTC Magazine (2004).

[3] IEC 61508: Functional safety of electrical/electronic/ programmable electronic safety-related systems. International Electrotechnical Commission, 2010.

[4] ISO 26262 - Road vehicles—Functional safety. International Organization for Standardization / Technical Committee 22 (ISO/TC 22), 2009.

[5] RTCA DO-178B. Software Considerations in Airborne Systems and Equipment Certification. Radio Technical Commission for Aeronautics (RTCA), 1992.

[6] J. Rushby: "Modular Certification", Technical report, NASA/CR-2002-212130, 2002.

[7] T. Willke, P. Tientrakool and N. Maxemchuk, "A Survey of Inter-Vehicle Communication Protocols and Their Applications," IEEE Communications Surveys & Tutorials, 11(2):3-20, 2009.

[8] "Autonomous Cars: Self-Driving the New Auto Industry Paradigm", Morgan Stanley report, November 6th, 2013.

[9] I. Keddie. "Analysis: UMVs set on course for naval service, Jane's Defence Weekly", 2012, HIS Global Ltd.

[10] ARTEMIS-IA, https://artemis-ia.eu/ 2015-02-13

[11] The Co-summit 2013: Bolstering Software innovation to foster hi-tech employment and industry opportunities https://itea3.org/ press/the-co-summit-2013-bolstering-software-innova.html, Published on 01 March 2014.

[12] Decision of The Governing Board of The ECSEL Joint Undertaking. Adopting the ECSEL Work Plan for the year 2014,ECSEL-GB-2014.07, http://ecsel.eu/web/downloads/ documents/ECSEL-GB-2014-07-workplan_v33.pdf 2015-02-13

[13] E. Armengaud, "The CESAR Reference Technology Platform (RTP) – and way beyond", presented at the ARTEMIS Spring Event, 13–14th of March, 2013, Brussels.

[14] Composition with Guarantees for High-integrity Embedded Software Components Assembly (CHESS), ARTEMIS project. http://www.chess-project.org/ 2016-12-23

[15] Guaranteed Component Assembly with Round Trip Analysis for Energy Efficient High-integrity Multi-core Systems (CONCERTO), ARTEMIS project. http://www.concerto-project.org/ 2016-12-23

[16] CHESS-toolset, https://www.polarsys.org/chess/ 2016-12-23

[17] OCRA: Othello Contracts Refinement Analysis. https://es-static.fbk.eu/ 2016-12-23

[18] ASCAD: The Adelard Safety Case Development Manual. http://www.adelard.com/services/SafetyCaseStructuring/ 2016-12-23

[19] GSN Community Standard Version 1. Technical report, Origin Consulting (York) Limited, November 2011.

[20] Object Management Group (OMG). SACM: Structured Assurance Case Metamodel. Technical Report, Version 2.0, OMG, 2016. http://www.omg.org/spec/SACM/ 2016-12-23

[21] I. Sourdis, C. Strydis, A. Armato, C.S. Bouganis, B. Falsafi, G.N. Gaydadjiev, S. Isaza, A. Malek, R. Mariani, D. Pnevmatikatos, and D.K. Pradhan. DeSyRe: On-demand system reliability. *Microprocessors and Microsystems*, *37*(8), pp.981-1001, 2013.

[22] A. Masrur, M. Kit, V. Matěna, T. Bureš, and W. Hardt. Component-based design of cyber-physical applications with safety-critical requirements. *Microprocessors and Microsystems*, *42*, pp.70-86, 2016.

[23] H. Kopetz, Real-Time Systems Design Principles for Distributed Embedded Applications. Norwell, MA: Kluwer, 1997.

Author Bio

Prof. Paul Pop received his Ph.D. degree in computer systems from Linköping University in 2003, he has been an associate professor at DTU Compute, Technical University of Denmark, and since 2016 he is a Professor of Cyber-Physical Systems. His research is focused on developing methods and tools for the analysis and optimization of dependable embedded systems. In this area, he has published over 130 peer-reviewed papers, 3 books and 7 book chapters. He and has received the best paper award at DATE 2005, RTIS 2007, CASES 2009, MECO 2013 and DSD 2016. He has also received the EDAA Outstanding Dissertations Award (co-supervisor) in 2011. His research has been highlighted as "The Most Influential Papers of 10 Years DATE". He is the director of DTU's IoT Research Center and has coordinated the Danish national InfinIT Safety-Critical Systems Interest Group. He is the chairman of the IEEE Danish Chapter on Embedded Systems. He has served as technical program committee member on several conferences, such as DATE and ESWEEK.

Detlef Scholle is a Program Manager of software engineering and development at Alten Sweden. Detlef has deep knowledge of real-time embedded systems, including small device components and large telecom systems.

Irfan Šljivo is a Ph.D. student at Mälardalen University, Västerås, Sweden. Irfan got his bachelor degree in Computer Science at Faculty of Electrical Engineering, University of Sarajevo, Bosnia and Herzegovina. In 2011 he graduated as M.Sc. in Artificial Intelligence from University of Sarajevo. After graduation he has started his PhD studies at Mälardalen University in 2012 . His research topics include usage of Safety Contracts to facilitate composable safety certification in order to reduce the cost incurred by the certification of safety-critical systems.

Hans Hansson is professor in Real-Time Systems at Mälardalen University since 1997. He is director of Mälardalen Real-Time Research Centre and the PROGRESS national strategic research centre, Scientific Leader of SICS Swedish ICT Västerås AB and the EU/ARTEMIS project SafeCer. He received an MSc (Engineering Physics), a Licentiate degree (Computer Systems), a BA (Business Administration), and a Doctor of Technology degree (Computer Systems) from Uppsala University (UU), Sweden, in 1981, 1984, 1984 and 1992. Prof. Hansson's previous appointments include being director of the nat'l research programme ARTES, visiting prof. and dept. chair at the Dept. of Computer Systems, Uppsala University, and researcher and scientific advisor at the Swedish Institute of Computer Science (SICS) in Stockholm.

Gunnar Widforss is Certified Project Manager (IPMA, International Project Management Association), expert evaluator at the European Commission and Member of the Professional Development Working Group in the European Association of Research Managers and Administrators (EARMA). Currently he coordinates the ECSEL-project MegaM@Rt2, manages a advocacy project (HoPiiA+) that promotes Swedish interests at the European Commission, and is also part of the management team of the Industrial Graduate School ITS EASY, as well of the research profile Dependable Platforms for Autonomous systems and Control (DPAC). He is also part of the AMASS-project and the coordination team of the SafeCOP-projects (ECSEL).

Malin Rosqvist is a senior project manager within Embedded Systems at the School of Innovation, Design and Engineering. Since joining MDH in 2009 she specializes in running projects and activities in cooperation with industry, as well as in research communication and public relations. Malin is board member of the non-profit organisation Swedsoft which was founded in 2007 in a joint venture between ABB, Ericsson, SAAB AB, Volvo AB and several universities in Sweden. She is the project manager of PROMPT (Professional Master's in Software Engineering).